REMARKS

In view of the amendments and the following reasoning for allowance, the applicants hereby respectfully request further examination and reconsideration of the subject application.

A. Claim Objections

Claim 16 is objected to because "using the a trusted computing device" was incorrect. The applicants have amended claim 16 to "using a trusted computing device" as suggested by the Examiner to overcome this objection.

B. The 35 USC 112 second paragraph Rejection of Claims 11,17-20 and 30-34.

Claims 11, 17-20 and 30-34 were rejected under 35 USC §112 second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter that the applicant regards as the invention. Claim 11 was rejected because of the limitation "said user's computing device" was alleged to have insufficient antecedent basis. The applicant has amended this claim "said" to "a" to overcome this rejection. Claim 19 was rejected because of incorrect claim dependency, the applicants have amended Claim 19 to depend from Claim 18 to overcome this rejection. Claims 17-20 and 30-34 were rejected because it was alleged that the term "significant" is indefinite. Claim 17 has been cancelled and Claim 30 has been amended to remove the "significant resources" language, rendering this rejection moot. Claims 21 and 22, depending from Claim 16, were rejected as having improper antecedent basis. Claims 16 has been amended to correct this problem.

It is believed that the above described amendments have placed the claims in condition to overcome the 35 USC 112 second paragraph rejection. Reconsideration of Claims 11, 17-20 and 30-34 is respectfully requested.

C. The 35 USC 101 Rejection of Claims 35-41.

Claims 35-41 were rejected under 35 USC §101 as allegedly being directed to non-statutory subject matter. More particularly, the Examiner stated that a "computer-readable medium" is non-statutory since "it is not limited to tangible embodiments." because the claimed invention is allegedly directed to non-statutory subject matter. More particularly, it was stated that the disclosed meaning of what the claimed computer readable medium may consist of, includes a modulated signal such as a carrier wave.

While the applicant does not admit to and does not believe that the aforementioned disclosed meaning is non-statutory subject matter, it has been decided to amend the specification to eliminate any reference to a computer readable medium including a modulated signal such as a carrier wave. The intent of the amendment to the specification is to limit the claimed invention to the use of *physical* computer readable media, and that the use of carrier waves is not intended to be included in the scope of the claimed invention.

In view of the amended specification, it is believed Claims 35-41are patentable under 35 USC 101. Therefore, it is respectfully requested that the rejection of this claim be reconsidered.

D. The 35 USC 102(e) Rejection of Claims 1-7, 10-13, 16, 17, 23, 35-38.

Claims 1-7, 10-13, 16, 17, 23, 35-38 were rejected under 35 USC 102(e) as being anticipated by Hsu et. al, U.S. Patent No. 6,038,666 herein after referred to as Hsu. It was contended in the above-identified Office Action that Hsu teaches all the elements of the rejected claims. The applicants have traversed this contention of anticipation.

The applicants' claimed invention is a technique for determining if a computer user is a human or a computer program such as an automated script. The technique does not require a user to interact with a service provider in order to obtain and answer a challenge. Thus, the embodiments of the claimed invention are advantageous in that they preclude the need for the great number of actions and time delays that are required for typical HIP systems where a service provider sends a challenge to a user, the user answers the challenge and sends their answer back to the service provider, and the service provider verifies the user's answer before allowing the user access to the service. Additionally, the claimed invention allows some of the HIP costs to be shifted to devices owned by the user or a dedicated third party instead of the service provider.

In general, in one embodiment, a computer user's computing device is equipped with a trusted computing environment or device consisting of a challenge generator and a secret key. The challenge is generated for the user by the user's trusted computing environment or device, and the user answers the challenge. A digital signature which may or may not include the user's answer, or may be appended to the user's answer, is provided as part of the user's service request to a service provider to access their services. For example, the digital signature can be appended to the message body (which may include such things as the correct answer, timestamp, request for services, and so on) to prove the authenticity and integrity of the message to the service provider. Such a signed assertion or signed message created by the trusted computing environment or device, or trusted third party in the case where one is employed, proves to the services provider that the user has completed the challenge. This obviates the need for a separate challenge to be generated and sent from the service provider and the user's response to that challenge being sent back to the service provider. It also significantly reduces the burden on the service provider. It should be noted that in any one of the embodiments a keyed hash can be used as an alternative to a digital signature. A keyed hash (a hash in which one of the inputs is a secret key) requires the authenticator to share a secret key with the entity being authenticated, so a digital signature is sometimes preferred.

In one embodiment of the claimed invention, the user's trusted computing environment computes a one-way cryptographic hash of the contents of a message using, for example, the date, the sender's name/address, the recipient's name/address, and the secret key. The result of the aforementioned hash is used to generate a short sequence of alphanumeric characters which can, for example, then be rendered into a visual image that is given to the user as a challenge. The user can then identify the text string as their answer to the challenge and include it with the mail message. A recipient, such as the service provider, with access to the same secret key can check that the included text string matches the hash of the message contents, date, etc., and reject the message if there is no match. This relieves the sender from the burden of having to wait for a challenge from the recipient and relieves the recipient from having to send the challenges. (Summary)

In contrast, Hsu discloses a technique for automatically verifying the identity of a person seeking access to a protected property that is remotely located with respect to the apparatus, such as a remotely located computer file or building alarm system. The apparatus, which is disclosed in the form of a handheld device or other portable device, includes a sensor for reading biometric data, such as a fingerprint image, from the person, and a correlator for comparing the sensed data with a previously stored reference image and for determining whether there is a match. If there is a match, the device initiates an exchange of signals over a communication network, with the "door" that protects the property. Specifically, the device generates a numerical value, such as a cyclic redundancy code, from the stored reference image, encrypts the numerical value, and transmits it to the door as confirmation of the person's identity. For further security, the person registers this numerical value at each door to which access is desired. Upon receipt of identity confirmation from the device, the door (10) compares the received numerical value with the one stored during registration, before granting access to the protected property. (Abstract)

Hsu, however, does not teach the applicants' claimed generating a challenge at a user's computing device comprising the actions of: (1) the user generating a preliminary request for services message to the service provider; (2) generating a

cryptographic hash using data from the preliminary request for services message; and (3) using said cryptographic hash to generate the challenge.

A prima facie case of anticipation is established only when the Examiner shows, inter alia, that the cited reference teaches each of the claimed elements of a rejected claim. In this case, the Hsu reference does not teach the advantageous features of the applicants' claimed invention such as not having to gather and use biometric data in order to verify a person's identity. Thus, the rejected claims recite advantageous features that are not taught in the cited art, and as such a prima facie case of anticipation is traversed with the claims as amended. It is, therefore, respectfully requested that the rejection of Claims 1-7, 10-13, 16, 17, 23, 35-38 be reconsidered based on the exemplary novel claim language:

> " A computer-implemented process for determining whether a computer user is a human or a computer program, comprising the process actions of:
>
> generating a request for services of a service provider at a user's computing device;
>
> generating a challenge at a user's computing device **comprising the actions of:**
>
> **the user generating a preliminary request for services message to said service provider;**
>
> **generating a cryptographic hash using data from said preliminary request for services message; and**
>
> **using said cryptographic hash to generate said challenge;**
>
> the user answering the challenge;
>
> said user's computing device evaluating said user's answer to the challenge and attaching a digital signature thereto if said user's answer is correct;
>
> sending said request for services including said digital signature from the user to a service provider;
>
> said service provider evaluating said user's request for services and digital signature; and
>
> said service provider determining whether to allow said user access to said service provider's services based on said evaluation of said digital signature." (emphasis added)

E. The 35 USC 102(e) Rejection of Claims 26-27.

Claims 26-27 were rejected under 35 USC 102(e) as being anticipated by McGarvey et al, U.S. Patent Application No. 20030028773 herein after referred to as

McGarvey. It was contended in the above-identified Office Action that McGarvey teaches all the elements of the rejected claims. The applicants have traversed this contention of anticipation.

As discussed above, in one embodiment of the applicant's claimed invention, a computer user's computing device is equipped with a trusted computing environment or device consisting of a challenge generator and a secret key. The challenge is generated for the user by the user's trusted computing environment or device, and the user answers the challenge. In one embodiment the user's trusted computing environment computes a one-way cryptographic hash of the contents of a message using, for example, the date, the sender's name/address, the recipient's name/address, and the secret key. The result of the aforementioned hash is used to generate a short sequence of alphanumeric characters which can, for example, then be rendered into a visual image that is given to the user as a challenge. The user can then identify the text string as their answer to the challenge and include it with the mail message. A recipient, such as the service provider, with access to the same secret key can check that the included text string matches the hash of the message contents, date, etc., and reject the message if there is no match.

In contrast, McGarvey discloses a technique to provide for a middle-tier server to impersonate a client to a plurality of servers. A common nonce associated with each of the plurality of servers is obtained and the common nonce to the client. The common nonce signed by the client is received at the middle-tier server and provided as a signature for transactions from the client to the plurality of servers so as to authenticate the client to the plurality of servers. (Abstract)

McGarvey, however, does not teach the applicants' claimed generating a challenge at a user's computing device comprising the actions of: (1) the user generating a preliminary request for services message to the service provider; (2) generating a cryptographic hash using data from the preliminary request for services message; and (3) using said cryptographic hash to generate the challenge.

A prima facie case of anticipation is established only when the Examiner shows, inter alia, that the cited reference teaches each of the claimed elements of a rejected claim. In this case, the McGarvey reference does not teach the advantageous features of the applicants' claimed invention such as being able to authenticate a user without using a middle tier server or biometric data **by generating a challenge by using a cryptographic hash.** Thus, the rejected claims recite advantageous features that are not taught in the cited art, and as such a prima facie case of anticipation is traversed with the claims as amended. It is, therefore, respectfully requested that the rejection of Claims 26-27 be reconsidered based on the exemplary novel claim language:

> " A computer-implemented process for determining whether to allow a computer user access to a service provider's services, comprising the process actions of:
>
> a user generating a preliminary request for services message to a trusted computing device resident at a trusted third party;
>
> **generating a challenge for the user that comprises a partial digital signature using the trusted computing device resident at the trusted third party by:**
>
> **generating a cryptographic hash using data from said preliminary request for services message; and**
>
> **using said cryptographic hash to generate said challenge;**
>
> the user answering the challenge to complete the digital signature;
>
> the user sending a request for services including the complete digital signature to a service provider;
>
> said service provider evaluating said user's request for services and digital signature; and
>
> said service provider determining whether to allow said user access to said service provider's services based on said evaluation of said user's request for services and digital signature. " (emphasis added)

F. The 35 USC 103 Rejection of Claims 28-30 and 33.

Claims 28-30 and 33 were rejected under 35 USC 103(a) as being unpatentable over Billingsley et al., U.S. Patent No. 7,139,916, hereinafter Billingsley, in view of Remer et al. (U.S. Patent No. 6,742,039), herein after Remer, in view of Stallings. The Examiner contended that though Billingsley does not teach using a third party to process verification of a user when the user requests access to a service provider, or including a digital signature in the request to a service provider Remer and Stalling

teach these features. The applicants respectfully traverse this contention of obviousness.

In order to deem the applicants' claimed invention unpatentable under 35 USC 103, a prima facie showing of obviousness must be made. To make a prima facie showing of obviousness, all of the claimed elements of an applicants' invention must be considered, especially when they are missing from the prior art. If a claimed element is not taught in the prior art and has advantages not appreciated by the prior art, then no prima facie case of obviousness exists. The Federal Circuit court has stated that it was error not to distinguish claims over a combination of prior art references where a material limitation in the claimed system and its purpose was not taught therein (*In Re Fine*, 837 F.2d 107, 5 USPQ2d 1596 (Fed. Cir. 1988)).

As discussed above, in one embodiment of the applicant's claimed invention, a computer user's computing device is equipped with a trusted computing environment or device consisting of a challenge generator and a secret key. The challenge is generated for the user by the user's trusted computing environment or device, and the user answers the challenge. In one embodiment the user's trusted computing environment computes a one-way cryptographic hash of the contents of a message using, for example, the date, the sender's name/address, the recipient's name/address, and the secret key. The result of the aforementioned hash is used to generate a short sequence of alphanumeric characters which can, for example, then be rendered into a visual image that is given to the user as a challenge. The user can then identify the text string as their answer to the challenge and include it with the mail message. A recipient, such as the service provider, with access to the same secret key can check that the included text string matches the hash of the message contents, date, etc., and reject the message if there is no match.

In contrast, Billingsley discloses a technique for monitoring the interaction between a user and a computer. The technique includes generating an image including random reference data readable by the user, and communicating the image to the computer for display to the user. User input data is then received and a

comparison between the random reference data and the user input data is performed to determine if the user is interacting with the computer.

Billingsley, however, does not teach the applicants' claimed generating a challenge at a user's computing device comprising the actions of: (1) the user generating a preliminary request for services message to the service provider; (2) generating a cryptographic hash using data from the preliminary request for services message; and (3) using said cryptographic hash to generate the challenge. Nor do Remer and Stallings teach these claimed limitations.

Accordingly, Billingsley in combination with Remer and Stallings does not teach the applicant's claimed using a cryptographic hash to generate a challenge. Nor does Billingsley in combination with Remer and Stallings recognize the advantages of the applicants' claimed invention, such as generating a challenge without using a middle tier server or biometric data.

Thus, the applicants have claimed elements not taught in the cited art and which have advantages, such as the ability of the remote viewer to control the presentation, not recognized therein. Accordingly, no prima facie case of obviousness has been established in accordance with the holding of *In Re Fine*. This lack of prima facie showing of obviousness means that the rejected claims are patentable under 35 USC 103 over Billingsley in view of Remer and Stallings. As such, it is respectfully requested that Claims 28-30 and 33 be allowed based on the following exemplary claim language:

> " A computer-implemented process for determining whether a computer user is a human or a computer program, comprising the process actions of:
>
> generating a request for services of a service provider at a user;
>
> generating a challenge at a trusted third party and providing it to said user comprising the actions of:
>
> **generating a cryptographic hash using data from the request for services; and**
>
> **using said cryptographic hash to generate said challenge;**
>
> the user answering the challenge;

said trusted third party evaluating said user's answer to the challenge and attaching a digital signature thereto if said user's answer is correct;

sending said request for services including said digital signature from the trusted third party to a service provider;

said service provider evaluating said user's request for services and digital signature; and

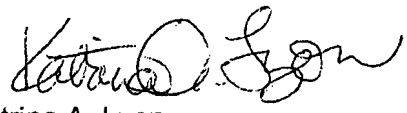
said service provider determining whether to allow said user access to said service provider's services based on said evaluation of said digital signature. " (emphasis added)

G. <u>Allowable Subject Matter of Claims 8, 9,14, 15, 24, 25.</u>

Claims 8, 9, 14, 15, 24 and 25 were objected to as being dependent upon a rejected base claim but were specified as being allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. The applicant gratefully acknowledges the allowability of these claims.

In summary, it is believed that the remaining Claims 1-7, 9-13, 15-16, 18-38 and 39-41 are in condition for allowance. Allowance of these claims at an early date is courteously solicited. The applicant kindly requests that the Examiner call the applicant at 805-278-8855 if he has any questions or concerns.

Respectfully submitted,



Katrina A. Lyon
Registration No. 42,821
Attorney for Applicants

LYON & HARR, LLP
300 Esplanade Drive, Suite 800
Oxnard, CA 93036
(805) 278-8855